COMUNICADO SINC N. 03/2017

A Seção de Segurança da Informação e Comunicação- SINC gostaria de auxiliá-los a identificar e-mails fraudulentos. As amostras abaixo são reais, recebidas por unidades administrativas e judiciárias do Tribunal.

Caso receba mensagens semelhantes às relatadas, envie o e-mail para a SINC tomar as providências cabíveis: sinc@trt3.jus.br.

Em sua maioria, as fraudes digitais cometidas por cibercriminosos visam obter dados pessoais e intransferíveis, como usuário e senha, dados de cartão de crédito, dados sigilosos de instituições, ou para instalar programas nos computadores visando solicitar o pagamento de resgate através da criptografia de informações (conforme noticiado na mídia mundial com o Ransomware WannaCry). Cada vez mais o e-mail é utilizado como passo inicial de grandes ataques, portanto, **frisamos os seguintes pontos fundamentais no uso da tecnologia:**

- ✓ **Não informe seu usuário e sua senha para ninguém,**
- ✓ **Não clique em links e nem faça download de arquivos de fontes desconhecidas,**
- ✓ **A senha de unidade administrativa ou judiciária é de responsabilidade do gestor. Somente ele deve ter conhecimento da senha. Caso queira delegar, utilize o recurso de delegação do Click,**
- ✓ **Troque sua senha com regularidade.**

Exemplo de identificação de e-mail malicioso 01 – 18/05/2017

De: Departamento de Informatica <avale@brhc.com.br>

Não existe tal e-mail e unidade no Tribunal.

Data: 18/05/2017 14:40

Assunto: Informações

Assunto Genérico

Erros de Português, frases desconexas advindas de traduções automáticas.

Estamos conduzindo nossa manutenção anual de atualização e webmail apagando assim toda conta de e-mail não utilizadas para criar espaço para a conta de email ativa e funcional. Você por este meio é aconselhado para validar a sua conta de e-mail webmail, então ele não será excluído como uma conta não utilizada.: Para atualizar sua conta de e-mail clique aqui

Link para redirecioná-lo ao site externo fraudulento que irá coletar seus dados ou infectar seu computador.

Nota: Sua conta será encerrada se você fornecer informações incorretas ou não conseguir validar sua conta de e-mail webmail dentro de 12 horas.

Ameaça para induzir o usuário ao erro e passar credibilidade.

Exemplo de identificação de e-mail malicioso 02 – 23/05/2017

De: Administrador do serviço de webmail <debora@finep.gov.br>

Não existe tal e-mail no Tribunal.

Data: 23/05/2017 11:33 AM

Assunto: Atenção

Assunto Genérico

A todos os usuário do webmail-estima

Erros de Português e frases desconexas advindas de traduções automáticas presente em todo o corpo do e-mail. Foram destacados em vermelho.

Isto é para notificar todos os nossos usuários de webmail que estamos atualizando nosso banco de dados webmail assim excluindo todos conta de webmail não utilizados para criar espaço para conta de webmail funcional e activa. Durante este período de atualização, pedimos a todos os usuários de webmail/e-mail para reconfirmar a sua conta de webmail com nosso administrador de forma a manter a sua conta de e-mail.

Para atualização imediata por favor confirmar detalhes abaixo

Neste caso as informações sigilosas , pessoais e intransferíveis são solicitadas no corpo do e-mail.

Nome:
E-mail:
Nome de usuário:
Senha:
Confirmar senha:
Número de telemóvel:

Ameaça para induzir o usuário ao erro.

Nota: assim que estas informações são recebidas, confirmando sua conta de e-mail está ativo e funcional, nós imediatamente devem atualizar sua conta de webmail e você vai continuar a desfrutar de nossos serviços ininterruptos.

Tentativa de passar credibilidade

Cumprimentos
Administrador do serviço de webmail

Exemplo de identificação de e-mail malicioso 03 – 05/06/2017

Para: Recipients <mauricio.cardoso@ipsemg.mg.gov.br>
De: "Administración" <mauricio.cardoso@ipsemg.mg.gov.br>
Data: 02/06/2017 11:12 AM
Assunto: Última Notificação

Não existe tal e-mail no Tribunal.

Assunto Genérico

Erros de Português e frases desconexas advindas de traduções automáticas presente em todo o corpo do e-mail. Foram destacados em vermelho.

Gostaríamos de informar que estamos **actualmente** a realizar a manutenção programada e atualização do nosso serviço de webmail e como resultado deste um vírus HTK4S foi detectado nas pastas da sua conta, e sua conta tem que ser atualizado para a nova F-Secure HTK4S anti-virus/anti-Spam versão 2017 para evitar danos aos seus arquivos importantes. Preencher as colunas abaixo e enviar de volta **ou a sua conta de e-mail será suspenso** temporariamente de nossos serviços.

Neste caso as informações sigilosas , pessoais e intransferíveis são solicitadas no corpo do e-mail.

1 - Usuário:.....
2 - Senha: .....
3 - Confirmar senha:.....
4 - Telefone:.....

Ameaça com erros de português e com texto truncado.

Não fazer isso dentro de 24 horas irá imediatamente tornar a sua conta de e-mail desativado do nosso banco de dados